| Notice of Allowability | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/652,454 | CHERITON, DAVID | |
| | Examiner | Art Unit | |
| | Michael J. Simitoski | 2134 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--***

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *after-final amendment of 5/10/2006*.

2. ☒ The allowed claim(s) is/are *1,3,4,6-8,10,11,14,15,17-21,23-27,29,30,35-38 and 42-46*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   **Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20060523* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Jacques Louis-Jacques

## DETAILED ACTION

1. The response of 5/10/2006 was received and considered.

2. Claims 1, 3-4, 6-8, 10-11, 14-15, 17-21, 23-27, 29-30, 35-38 & 42-46 are allowed.

3. An Examiner's amendment begins on p. 3.

4. The Examiner's reasons for allowance being on p. 4.

## EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Cindy Kaplan (408-399-5608) on 5/19/2006.

The application has been amended as follows:

a. Please delete the word "medium" from **line 18 of claim 15**.

b. Please replace the word "refining" with "refines" in **line 12 of claim 44**.

6. The following is an examiner's statement of reasons for allowance:

c. Regarding claims 1, 15 & 44, Romig discloses separating data into a plurality of network flows (p. 2, ¶4-6), creating separate aggregate network flow summaries/flow logs for each of said network flows (p. 3, ¶1), sending at least one of said aggregate network flow summaries to a flow analyzer/Flow-dscan (p. 5, ¶1), analyzing said at least one aggregate network flow summary (p. 5, ¶1) to detect characteristics of potentially harmful network flows (p. 5, ¶1) and selecting a new aggregate network flow summary to analyze (p. 5, ¶2). Smith discloses generating a filter (a processing rule) and refining the filter (adding additional rules) (pp. 494, 496 & 498). However, Romig, as modified above, discloses performing the analysis at more powerful system, rather than at the network device and discloses sending additional flow summaries to an analyzer, hence lacking sending the selected aggregate network flow summary to the flow analyzer for analysis, wherein the new aggregate flow summary explicitly corresponds to network flow associated with the generated or refined filter.

d. Regarding claim 18, Romig discloses a netflow device operable to receive streams of packets, separate said streams (p. 2, ¶4-6), and create a summary record/flow logs containing information on each of said streams (p. 3, ¶1), a flow analyzer/Flow-dscan (p. 5, ¶1) operable to receive said summary records/Flow logs from said netflow device and analyze said summary records and identify potentially harmful network flows (p. 5, ¶1). Smith discloses generating a filter (a processing rule) (pp. 494, 496 & 498). However, Romig, as modified above, discloses performing the analysis at more powerful system, rather than at the network device and discloses creating new summary records of flows

removed from the cache, hence lacking the netflow device being operable to create a new summary record explicitly containing information on a stream of data associated with said generated or refined filter.

e. Regarding claim 30, the prior art relied upon fails to teach or suggest generating filters specifically for a corresponding network flow, refining the filter and modifying the classification of flows, in combination with the other elements of the claims.

f. The remaining claims are allowed based on their dependence upon the allowed claims discussed above.

7. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Conclusion***

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached at (571) 272-6962.

**Any response to this action should be mailed to:**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
**Or faxed to:**
(571) 273-8300
(for formal communications intended for entry)
**Or:**
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS

May 17, 2006